OFFICE OF THE WHISTLEBLOWER OMBUDS

May 2022

INTELLIGENCE COMMUNITY WHISTLEBLOWING

OVERVIEW

Executive branch employees and contractors who work within, or are assigned to, elements of the U.S. Intelligence Community (IC) have unique processes for making protected whistleblower disclosures to specific audiences. They rely on limited, **administrative processes** to enforce their rights against retaliation.

The legal framework is complex, in part because of rules that govern the handling and disclosure of classified information. Mishandling of such information, or disclosing it without authorization, can lead to administrative sanctions as well as criminal penalties. Those contemplating making such a disclosure should consider consulting **knowledgeable counsel**, including – to the extent a matter may implicate classified information – counsel holding the necessary security clearance.

INTELLIGENCE COMMUNITY WHISTLEBLOWING

Federal employees and contractors working for one of the **18 elements** of the IC are excluded from protections under the Whistleblower Protection Act, the primary executive branch whistleblower law, and from non-IC federal contractor protection laws. Instead, other federal statutes and policies authorize IC whistleblowers to make disclosures to certain authorities and, under certain circumstances, furnish protection for IC whistleblowers from reprisal for making such disclosures.

IDENTIFYING THE 18 "ELEMENTS" AND THEIR PROTECTED EMPLOYEES

The 18 elements of the intelligence community include independent agencies but are mainly comprised of intelligence departments within non-IC agencies and the military branches:

- Office of the Director of National Intelligence
- Central Intelligence Agency
- Defense Intelligence Agency
- National Security Agency
- National Geospatial Intelligence Agency
- National Reconnaissance Office
- Federal Bureau of Investigation
- The intelligence elements of the Army, Navy, Coast Guard, Marine Corps, Air Force, and Space Force
- The Department of Energy's Office of Intelligence and Counterintelligence
- The Department of Homeland Security's Office of Intelligence and Analysis
- The Drug Enforcement Agency's Office of National Security Intelligence
- The Department of State's Bureau of Intelligence and Research
- The Department of the Treasury's Office of Intelligence and Analysis

Note that while the **Federal Bureau of Investigation** (FBI) is considered to be an element of the IC, FBI employees are **excluded** from the IC whistleblowing protections discussed below and rely instead on their own unique statute at 5 U.S.C. § 2303.

Similarly, while the intelligence elements of the **armed forces** are also considered to be elements of the IC, their unique protections are outlined in the Military Whistleblower Protection Act. (10 U.S.C. § 1034).

A "PATCHWORK" OF PROTECTIONS

Various laws, orders, and other directives may apply to IC personnel who wish to blow the whistle, depending on the circumstances.

Congress established the primary relevant laws through the **Intelligence Community Whistleblower Protection Act of 1998**, and the **Intelligence Authorization Acts for Fiscal Years 2010 and 2014**. Together with other laws, these define the boundaries of a protected disclosure and outlaw retaliation against covered employees. Further, the relevant enforcement processes are laid out in **Presidential Policy Directive 19 (PPD-19), Intelligence Community Directive 120 (ICD-120),** and in individual agency policies.

PROTECTED DISCLOSURES

There are several statutes that outline the required processes and approved audiences for IC whistleblower disclosures.

ELEMENTS OF A PROTECTED DISCLOSURE

Pursuant to the **National Security Act**, it is unlawful to retaliate against an IC employee, contractor, subcontractor, subgrantee, or personal services contractor because of their protected whistleblowing disclosure. (50 U.S.C. § 3234).

The statute defines a protected disclosure as a **lawful disclosure** of information that the covered employee **reasonably believes** evidences any of the following misconduct:

- A violation of any federal law, rule, or regulation
- Mismanagement
- A gross waste of funds
- An abuse of authority
- A substantial and specific danger to public health or safety

By statute and other authorities, in order to be protected**, disclosures** may only be made to:

- The Director of National Intelligence (DNI) or their designee
- The Inspector General of the Intelligence Community (ICIG)
- A supervisor in the whistleblower's direct chain of command
- A supervisor in the relevant agency with responsibility for the subject matter of the disclosure, up to and including the head of the agency or their designee
- The inspector general (IG) of the relevant agency
- A congressional intelligence committee or any member of those committees

The law also prohibits retaliation against lawful disclosures made in conjunction with **certain activities**:

- The exercise of any appeal, complaint, or grievance right
- Testimony for, or lawfully assisting any individual with, their own appeal, complaint, or grievance right
- Cooperation with, or disclosures made to, an inspector general in connection with the IG's audit, inspection, or investigation

A NOTE ON CLASSIFIED INFORMATION

While not all disclosures from IC whistleblowers involve classified information, disclosures involving classified information can only be made through secure channels and between individuals who are authorized to receive the disclosures.

As a co-equal branch of government, **Congress takes the position that it can lawfully receive classified disclosures** that are communicated through the proper channels. **Still, the executive branch does not agree that whistleblowers' disclosures can be made directly to Congress in every instance, even when not classified.** As such, there is a risk that whistleblowers could experience adverse security clearance actions or other serious consequences for disclosing information. Knowledgeable counsel for the IC whistleblower and the recipient of their disclosure is advised.

DISCLOSING AN "URGENT CONCERN" TO CONGRESS

IC employees, contractors, assignees, and detailees may also disclose matters of "**urgent concern**" to the congressional intelligence committees through the ICIG or their agency's (or contracting agency's) IG. **Such disclosures are protected** under the National Security Act. (50 U.S.C. § 3234(b)(2); (c)(1)(B)).

Once the OIG receives the urgent concern disclosure, the IG determines within **14 days**:

- The **credibility** of the disclosure, and
- Whether it qualifies as an **urgent concern** under the statutory definition

If the disclosure passes those tests, it is then sent on to the relevant agency head. The agency head then transmits the disclosure to the congressional intelligence committees within **seven days**.

If, for whatever reason, the IG fails to transmit the disclosure to the agency head, the whistleblower can send their disclosure to the intelligence committees directly. However, they must inform the IG that they are doing so and must receive and follow instructions on how to securely transmit the information to Congress.

DEFINING AN URGENT CONCERN

The **Intelligence Community Whistleblower Protection Act (ICWPA)** defines an urgent concern as:

- A serious or flagrant problem, abuse, violation of law or Executive order, or deficiency relating to the funding, administration, or operations of an intelligence activity involving classified information, but does not include differences of opinions concerning public policy matters;
- A false statement to Congress, or a willful withholding from Congress, on an issue of material fact relating to the funding, administration, or operation of an intelligence activity; or
- An action, including a personnel action described in section 2302(a)(2)(A) of title 5 constituting reprisal or threat of reprisal prohibited under section 7(c) in response to an employee's reporting an urgent concern in accordance with this section.

These processes are codified in the ICWPA at 50 U.S.C. § 3033; in the Inspector General Act at 5 U.S.C. App. § 8H; and in the CIA Act at 50 U.S.C. § 3517.

ENFORCEMENT OF RIGHTS AGAINST WHISTLEBLOWER RETALIATION

Although the National Security Act prohibits retaliation against protected whistleblowing and urgent concern disclosures, the law does not explicitly dictate procedures for enforcement. (50 U.S.C. § 3234(d)). Instead, the law requires that the president provide a means of enforcement that is as consistent as possible with the Whistleblower Protection Act.

Accordingly, whistleblowers must look to agency-specific provisions created under Presidential Policy Directive-19 (PPD-19), which was interpreted through Intelligence Community Directive-120 (ICD-120), for processes on enforcing their rights.

PPD-19: PROCESS FOR SEEKING RELIEF AGAINST WHISTLEBLOWER RETALIATION

Created in 2012, PPD-19 outlines an administrative (i.e. non-judicial) process for covered IC employees to seek enforcement of their whistleblowing rights. ICD-120 interprets the application of PPD-19 to the IC elements.

Note that PPD-19 is a **presidential directive**, not a law. It directs each IC element to create and enforce its own policy in accordance with PPD-19's guidelines. PPD-19 also outlines an enforcement process for security clearance retaliation, discussed more below.

PPD-19 PART A – INSPECTOR GENERAL INVESTIGATION AND AGENCY-HEAD DECISION

The enforcement process begins in Part A of PPD-19 with an **investigation** into the whistleblower's retaliation complaint by their agency's IG. After investigating, the IG will determine whether the whistleblower experienced prohibited retaliation and will **send a report** of the IG's findings to the head of the IC element agency involved. The IG may also recommend corrective action if they find there was retaliation (e.g. reinstatement, costs, and back pay, among other potential relief).

Importantly, **the IG's decision is not binding** on the agency. Rather, the **agency head** considers the IG report and makes the final decision on whether to order relief for the whistleblower and/or corrective action regarding the retaliator(s).

PPD-19 PART C – EXTERNAL REVIEW PANEL PROCESS (ADMINISTRATIVE APPEAL)

The whistleblower can administratively appeal an unfavorable initial decision to the ICIG by requesting an external review panel made up of three IGs, including the ICIG.

Note that the **ICIG has the discretion not to convene the panel**. If convened, the panel has **six months** to investigate the whistleblower's retaliation claim and either agree or disagree with the initial IG decision in a new report.

If the panel finds that the whistleblower faced unlawful retaliation, the panel sends its report to the head of the whistleblower's agency, who must consider the panel's findings and make the final determination of whether to order relief for the whistleblower. Note that the external review panel's **findings and recommendations are not binding** on the agency head.

A NOTE ON FEDERAL CONTRACTORS AND GRANTEES

The National Security Act prohibits whistleblower retaliation against IC contractors and grantees (50 U.S.C. § 3234(c)). However, PPD-19's coverage of these individuals has been limited to Part B – which only deals with security clearance actions.

SECURITY CLEARANCE RETALIATION

The **Intelligence Reform and Terrorism Prevention Act** prohibits retaliatory security clearance actions in response to any lawful whistleblower disclosure. (50 U.S.C. § 3341(j)). PPD-19 Part B and ICD-120 Section F also cover retaliatory security clearance actions, and the PPD-19 Part C appeals process, as described above, is available to challenge an unfavorable initial decision.

A RETALIATORY CLEARANCE ACTION

The law prohibits those with authority from **taking, failing to take, or threatening to take** any action with respect to an employee's security clearance, or their access to classified information, in retaliation for the employee's lawful whistleblowing.

The law protects federal employees of an IC element, including FBI employees, as well as contractors, subcontractors, grantees, subgrantees, and personal services contractors. (50 U.S.C. § 3341(j)(8)).

ENFORCEMENT OF RIGHTS AGAINST RETALIATORY CLEARANCE ACTIONS

As with other IC whistleblowing matters, enforcement is administrative; there is no judicial review of a retaliatory clearance action (See: *Department of the Navy v. Egan,* 484 U.S. 518 (U.S. Sup. Ct.1988)). In fact, the law expressly prohibits any judicial review or private right of action. (50 U.S.C. § 3341(j)(7)-(8)).

Rather, employees must file complaints of clearance-related retaliation with the agency OIG. To succeed in their claim, whistleblowers must demonstrate that their lawful whistleblowing was a **"contributing factor"** in their revoked clearance or access. If they meet that standard, the defending agency must demonstrate by a **preponderance of the evidence** that it would have taken the clearance action in the absence of the whistleblowing—in other words, that its actions were legitimate. The statute also affords the **"utmost deference"** to the agency's assessment of the national security threat. (50 U.S.C. § 3341(j)(4)(C)).

Where a whistleblower is not successful in their claim and receives an unfavorable decision, they may appeal the decision to the Director of National Intelligence **within 60 days**.

DISPARATE BURDENS OF PROOF

Note that while this law instructs the president to enforce it in accordance with the Whistleblower Protection Act (WPA) to the fullest extent possible, it nevertheless applies a **comparatively lower bar** for the agency to defeat the whistleblower's retaliation claim. By contrast, the WPA requires agencies to meet the higher "clear and convincing" standard when defending personnel actions as legitimate. (5 U.S.C. § 1221(e)(2)).

TIMING MATTERS

Employees generally have **90 days** to file their allegation of a retaliatory security clearance action or access determination unless they can demonstrate good cause for a late filing. Further, if an employee is facing a suspension of their clearance or access, rather than a revocation, that **suspension must be for at least one year** for the employee to be able to challenge the action as unlawful clearance retaliation. (50 U.S.C. § 3341(j)(4)(A)).

WHISTLEBLOWER PROTECTION ACT AND CLASSIFIED DISCLOSURES

While employees and contractors of the 18 intelligence community elements are not protected under the Whistleblower Protection Act (WPA), certain employees who are covered under the WPA also have access to classified information and can make classified disclosures to Congress. (5 U.S.C. § 2302(b)(8)(C)(ii)).

Such disclosures are permitted if the information they are disclosing:

- **Was classified by the head of an agency that is not one of the 18 elements of the IC, and**
- **Does not reveal intelligence sources and methods**

Note, however, that disclosures still must be made through authorized channels and to authorized recipients. Whistleblowers could not, for example, send classified information through an online intake form of a Member of Congress that was designed to receive only unclassified disclosures. According to the Congressional Research Service (see pages 69-70), Members of Congress may generally access classified information without a security clearance, but congressional staff cannot.

PROTECTIONS FOR FBI EMPLOYEES

Employees of the Federal Bureau of Investigation (FBI) are excluded from the non-clearance related IC whistleblowing protections discussed above. Rather, they are covered under the **FBI Whistleblower Protection Enhancement Act,** codified at 5 U.S.C. § 2303. Note that FBI contractors are covered under the National Security Act, discussed above.

Under the Act, FBI employees can disclose evidence of misconduct that they **reasonably believe** evidences:

- A violation of any Federal law, rule, or regulation
- Gross mismanagement
- A gross waste of funds
- An abuse of authority
- A substantial and specific danger to public health or safety

The **protected audiences** for these disclosures are:

- The employee's chain of command
- The Justice Department Office of Inspector General
- Congress
- The Office of Special Counsel
- The Offices of Professional Responsibility of the Justice Department and FBI
- The FBI Inspection Division

Note that like other IC employees, FBI employees must use internal, **administrative processes** to enforce their rights. They may file a complaint with either the Justice Department Office of Inspector General or the Office of Professional Responsibility.

RESOURCES

- CRS report on intelligence community whistleblower protections
- ODNI IC whistleblowing overview
- ODNI External Review Panel procedures (i.e. policies implementing PPD-19 Part C)
- Oversight.gov "Whistleblower Protections for Employees with Security Clearances"
- DoD memorandum interpreting PPD-19
- Executive Order 12968 on Access to Classified Information
- Department of Justice Overview of FBI whistleblowing rights
- ICIG Report on Intelligence Community Whistleblower Matters & Harmonization of Processes and Procedures